31st Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 13-14, 2015

SOFTWARE ASSURANCE CHALLENGES FOR THE COMMERCIAL CREW PROGRAM

Patrick Cuyno
TASC, Patrick.Cuyno-1@nasa.gov

Kathy D. Malnick
WVHTC, Kathy.D.Malnick@ivv.nasa.gov
Chad E. Schaeffer
NASA, Chad.E.Schaeffer@nasa.gov

ABSTRACT

This paper will provide a description of some of the challenges NASA is facing in providing software assurance within the new commercial space services paradigm, namely with the Commercial Crew Program (CCP). The CCP will establish safe, reliable, and affordable access to the International Space Station (ISS) by purchasing a ride from commercial companies. The CCP providers have varying experience with software development in safety-critical space systems. NASA's role in providing effective software assurance support to the CCP providers is critical to the success of CCP.

These challenges include funding multiple vehicles that execute in parallel and have different rules of engagement, multiple providers with unique proprietary concerns, providing equivalent guidance to all providers, permitting alternates to NASA standards, and a large number of diverse stakeholders. It is expected that these challenges will exist in future programs, especially if the CCP paradigm proves successful.

The proposed CCP approach to address these challenges includes a risk-based assessment with varying degrees of engagement and a distributed assurance model. This presentation will describe NASA IV&V Program's software assurance support and responses to these challenges.

COMMERCIAL CREW PROGRAM (CCP) OVERVIEW

The Commercial Crew Program is a competitive program to transport crew to/from the International Space Station (ISS) using commercial provider services, not NASA provided, and is managed at Kennedy Space Center with support from around the Agency. It is a highly visible program that has the attention of the Agency. It attracts a lot of media attention and pressure given the goal of returning the capability to transport crew to/from the ISS from American launch sites.

The CCP uses multiple development phases governed by different “contract” vehicles (e.g., Space Act Agreements (SAA), formal contracts). The use of different agreement types for each phase allows for varied flexibility in the relationship between the providers and NASA. SAAs form partnerships that allow flexibility in the interactions between the commercial providers and NASA. Contracts are acquirer-provider agreements with specific rules for engagement. Funding multiple, parallel development efforts fosters competition which can result in lower prices for NASA as well as the potential for multiple service providers (i.e., redundancy). The Program requirements given to the providers are focused on what is to be built and not how the providers are to build the product resulting in fewer levied requirements. This allows commercial space providers to identify potentially more efficient/cost effective designs and processes and permits the use of approved alternate standards for some levied requirements.

Exhibit 1 below show the evolution of the various development phases, including the associated agreement types and the number of competing providers.

PHASE	DATE	PROVIDERS	CONTRACT TYPE	FOCUS
CCDev1 = Commercial Crew Development Round 1	2010	5	Space Act Agreement	Develop commercial crew transportation concepts and enabling capabilities
CCDev2 = Commercial Crew Development Round 2	2011-2013	4 Funded 3 Unfunded	Space Act Agreement	Design, development, test, review of systems
CCiCap = Commercial Crew Integrated Capability	8/2012-2014	3	Space Act Agreement	Perform tests and mature integrated designs
CPC = Certification Products Contract	12/2012-2014	3	Contract	1) Develop products to implement NASA flight safety and performance requirements; 2) Develop certification plan to achieve safe, crewed missions to the space station
CCtCap = Commercial Crew Transportation Capability	2014-2017	2	Contract	Final development, testing, verifications to allow crewed demonstration flights to ISS

Exhibit 1: Commercial Crew Development Phases

SMA SUPPORT OFFICE (SSO) SUPPORT

The SMA Support Office (SSO) supports the CCP Safety & Mission Assurance (SMA) Office to provide software expertise and software assurance reach-back support for the CCP SMA team. The main areas of provided assistance are assessing alternate standards and hazard reports. Under CCP, providers are given the option to provide NASA with alternates to standards typically levied on NASA projects. These standards require NASA approval before they can be used, therefore, an assessment process is used and the SSO provided assistance for assessments of standards related to software. In addition to these support activities, at the request of the CCP SMA team, SSO provides support for verification reviews, other plan reviews, review board support, etc.

SSO joined the CCP in the middle of the CCiCap phase, but at beginning of CPC (recall that phases overlapped) providing support for both CCiCap and CPC phases with plans to continue support through the CCtCap phase. In addition to the alternate standard assessments described above, SSO also assesses hazard reports. Given SSO's software background, the group focuses on the large number of hazard reports from each provider that include (or should include) software content. At the time of the original presentation in the fall of 2014, SSO had submitted comments to the program and providers with a 99% acceptance rate.

SOFTWARE ASSURANCE CHALLENGES

Software Assurance for CCP has a lot of challenges. This paper focuses on the key challenges faced by the SSO. These challenges are listed below and will be addressed separately.

- Atypical approach
- Large effort with multiple commercial solutions
- Keeping proprietary data separate
- Different funding methods with different rules
- Multiple phases with some running concurrently
- Multiple NASA stakeholders and projects with similar goals

The authors are not speaking for the Program who may have different or similar solutions for the challenges covered in this paper.

Atypical Approach

As mentioned earlier, a unique, atypical requirements approach that focused on the "what" rather than "how" is being used for the CCP. Among other things, this approach allows the providers to use approved alternates to NASA standards, to obtain waivers to specific requirements, and to use their own unique development methods and processes. This is a new experience for NASA since most NASA projects are governed by NASA standards, processes, methods, etc. A related challenge is that each provider has varying levels of experience working with NASA. Some have worked with NASA for years while, for other providers, this was their first experience working with NASA.

It was very challenging to adapt NASA software assurance approaches for this new environment. As stated earlier, one of the challenges of assessing alternate standards is that NASA must assess and approve those alternate standards and determine if they meet the full intent of the original NASA requirements. NASA received various types of artifacts submitted as alternate standards. A provider could deliver a single document or they could deliver a set of development plans, internal processes and requirement documents.

NASA had no formal approach for assessing these alternate standards, so SSO worked with the CCP SMA team to create one that focused on NASA software engineering, software assurance, and software safety requirements. The basic method, captured in a spreadsheet and used consistently across all -providers by the SSO, was:

- Identify evaluation criteria for the NASA requirements based on requirement rationale in the NASA standards and guidebooks
- Prioritize the NASA requirements via "risk-type" methodology:
    - Not relevant (e.g., software engineering requirements levied on NASA Headquarters or NASA Centers
    - High priority/risk (e.g., related to crew safety as opposed to cost or schedule)
    - Etc.
- Map the provider alternate standard, regardless of whether the standard was contained in one or more documents, to NASA requirements
- Evaluate mapped requirements, requirement by requirement using the pre-determined evaluation criteria capturing the "map" of where the NASA requirements were addressed in the provider documents
- Identify the gaps qualifying the associated risk for the CCP

The goal was to be flexible and allow as much freedom as possible to the providers while minimizing or eliminating additional risk to NASA. Some provider development approaches are dramatically different than traditional approaches. These differences add an additional dimension of complexity when mapping provider alternate standards[1] to NASA requirements.

Large Effort with Multiple Commercial Solutions

Prior to the CCtCap phase, there were multiple large, complex systems from multiple providers, each with different solutions, to understand and be assessed by a small, distributed SMA team. Since the core CCP SMA team is smaller than NASA typically assigns to a program of this size, the solution to is to focus and prioritize our efforts on the key critical areas (target software related content, crew safety, high risk areas) and use "risk-type" methodology to identify what matters and key areas on which to focus. To complete the required work using this small team, the team identified minimum success criteria and stretch goals. Stretch goals were applied only if the

team completed the minimum success criteria and had the bandwidth to perform the additional work. This allowed the team to be successful while providing the opportunity to exceed expectations.

A related challenge is that the SSO team is distributed across multiple NASA Centers adding coordination and scheduling challenges to completing the assigned work. To address this challenge, the team developed a technical reference and links to pertinent artifacts pulled from design details from past deliveries and spoke with Subject Matter Experts (SMEs) to obtain needed system understanding which was shared with all team members regardless of their work location. The team also uses a robust issue and comment tracking system that is accessible by all team members and provides progress tracking and issue updates. This system makes it easier to identify comments/findings for verification when the team receives revised documents from the providers and enables easy information export for CCP to review and import into their tracking system.

Keeping Proprietary Data Separate

Protecting proprietary data is a major challenge with one small team providing assurance to multiple providers. Extreme caution has to be taken when performing analysis and during discussions (e.g., teleconferences, review boards, etc.) to prevent cross-pollination of proprietary information across various providers.

As a solution, the CCP limits access to provider data to certain points of contact (POCs). However, with such a small team, it is not feasible for the SSO to firewall people entirely and the SSO initially struggled to gain access for all members of the team and had to resort to naming one POC per provider. SSO uses multiple methods to protect provider data, including firewalls and processes specific to data protection. Additionally, provider artifacts are maintained in the CCP repository (not stored locally), sensitive analysis data is stored in protected locations with restricted access, and analysis work products are separated by provider.

Different Funding Methods with Different Rules

CCP is using a combination of different funding methods (rules of engagement) such as Space Act Agreements (CCiCap) and contracts (CPC), each of which has different interaction rules. CCiCap work was performed under a Space Act Agreements (SAAs) and CPC work was performed under a contract. The premise for using SAAs is that SAAs allow NASA to help the providers improve their products by providing suggested improvements, not providing directives. When contracts are used, NASA's role is essentially to grade the product, summarize the risk to NASA, and deliver issues to the providers. With multiple concurring CCP phases, it was important for SSO to interact with the providers in accordance with the relevant type of agreement. Another factor that complicated interactions with the providers is that during CCtCap contract selection, a blackout period occurred while CCiCap and CPC milestones were occurring. This required SSO to ensure discussions and guidance were strictly focused on delivered artifacts and kept within the scope of those milestones.

To ensure these challenges were met, a rigorous peer review process involving both SSO and CCP SMA was performed to confirm that rules were being followed. SSO peer-reviewed analysis findings were provided to SSO's CCP SMA POC to perform his own review and, subsequently, share with the provider at his discretion and through available channels. The robust tracking system was also used in which analysis findings were captured as issues and recommendations with associated impact statements. This tracking system allowed SSO to support both sets of agreement rules for suggesting improvements or simply identifying issues and associated risks. To ensure that direct provider communications were focused appropriately, SSO asked questions to expose potential defects rather than simply stating issues.

Multiple Phases with Some Running Concurrently

CCP uses multiple phases executing concurrently. This has resulted in the same artifacts being delivered multiple times for assessment under different rules (those appropriate to the agreement governing that CCP phase). This sometimes resulted in SSO reporting the same issue more than once, but in different formats. For example, at one milestone SSO provided a recommendation for an analysis finding and at a separate milestone under a different agreement type, SSO documented the same finding as an issue. In our tracking system, SSO does

not track that as two separate comments. In addition to comment tracking, another aspect of this challenge is that it is possible for an "old" version of an artifact to be delivered in one phase when a newer version exists in another phase.

To address these challenges, SSO ensures that analysis work products persist across all CCP phases so that findings are not duplicated; if a finding is identified once, the analysis results capture it. Those persistent work products allow past comments to be verified, updated, and assessed for each subsequent version of the artifact. Analysis work products also capture and maintain the history (e.g., versions assessed, CCP phase in which each artifact was assessed) and current state of each evaluated artifact. All SSO analysis results are evidence-based (e.g., use specific references in provider documents as basis for conclusions and findings), focused on the changes in the assessed artifacts (e.g., identified by creating comparison reports using software tools such as BeyondCompare, etc.), and tailored based on the "rules" for the specific CCP phase.

Multiple NASA Stakeholders and Projects with Similar Goal

The CCP has multiple distributed and diverse stakeholders, but other NASA crewed programs have similar requirements and goals. Given this paradigm, there is a risk of inconsistent direction or interpretation of guidance across the various crewed programs. Programs such as NASA's Multi-Purpose Crew Vehicle (MPCV) has a similar set of a requirements to the CCP, but may have interpreted them differently.

To address this challenge, SSO focuses heavily on establishing and maintaining communication with the SSO team as well as with SSO's CCP SMA POC (e.g., added onsite SSO representative at Kennedy Space Center, hold periodic face-to-face meetings). SSO documents thought papers to facilitate communication within CCP SMA as well as across NASA programs (e.g., share these papers with MPCV). SSO uses pre-determined criteria to keep assessments consistent (e.g., the alternate standards spreadsheets described in the **Atypical Approach** section of this paper).

The CCP Providers and Suppliers are shown in Exhibit 2.

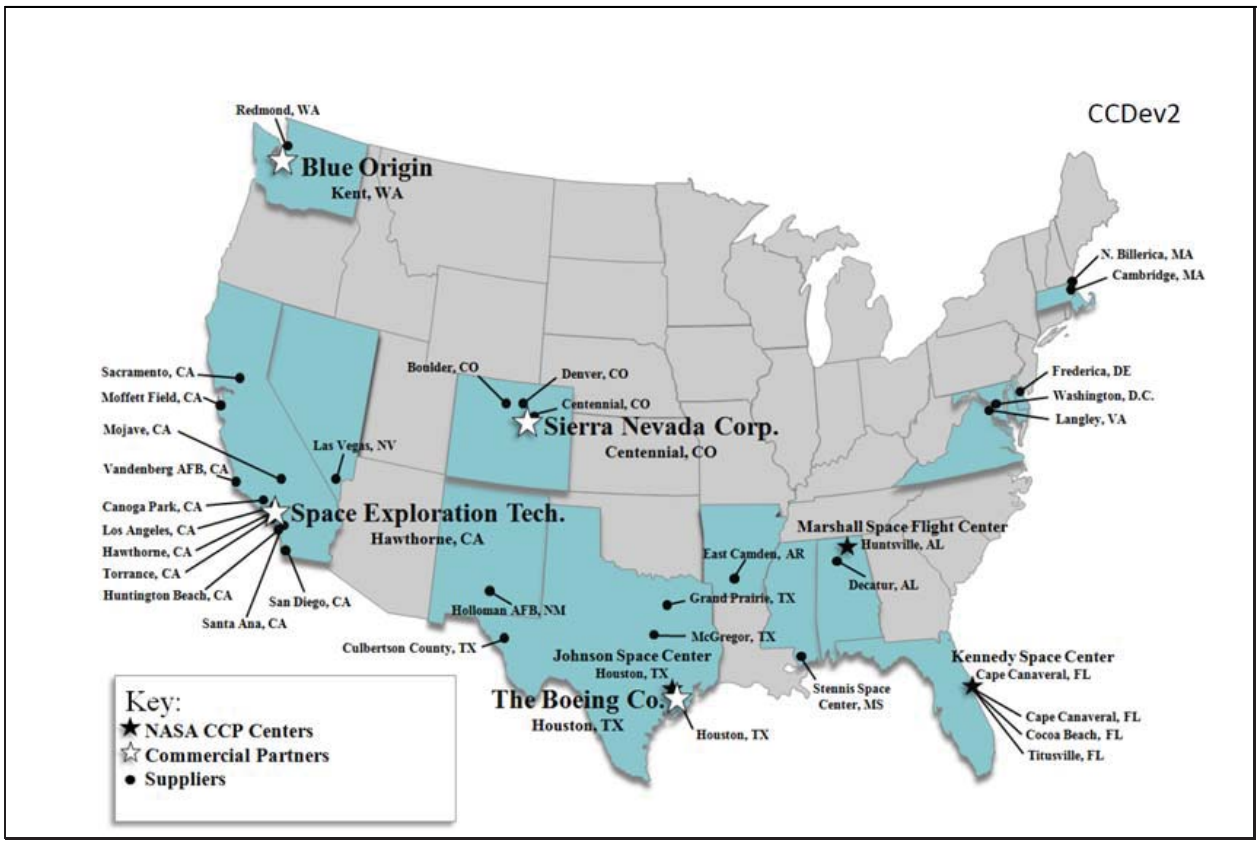


Exhibit 2: CCP Providers and Suppliers[2]

Other Challenges

In addition to the key challenges described above, the SSO experienced other challenges during support of the CCP CCiCap and CPC phases. Reviews were focused on delivered artifacts rather than program goals and standards. This meant that findings had to be provided per delivered artifact rather than on whether the provider met a goal or objective based on assessment of multiple artifacts. Artifact-focused assessments also made it difficult to assess and communicate the big picture; for example, the CCP repository did not have a field to input findings on the overall intent of meeting NASA's software engineering requirements. To address this challenge, in addition to providing findings on artifacts, the SSO provided summaries and additional feedback on bigger picture items such as hazard gaps and NASA software engineering standard compliance.

There were also limited processes/templates to perform the assessments, including no NASA definition or process for assessing "meets the intent" and no process for how to assess hazard reports for the CCP. To address this challenge, the SSO defined new processes and assets, developed evidence-based assessment criteria, and ensured all Providers received identical assessments.

Another challenge still facing SSO is that timeframes for analysis are shortened due to last-minute deliveries from providers and dynamic assignments to SSO by the CCP. To reduce the impact of this situation, the SSO has set up analysis processes to ensure that minimum success criteria are met when possible, continues to prioritize and scope each analysis effort, proactively monitors for support opportunities and assignments (e.g., sets up watches on pages of the CCP repository), and tries to meet the CCP's needs in addition to what they request (e.g., complete hazard report stretch goals, generate thought papers).

SUMMARY

Not all of the challenges presented in this paper were unexpected and most have been/are being met by the SSO using the solutions presented here. As solutions to challenges are developed, they are shared with the CCP. In spite of the challenges encountered, the experience of the SSO has shown that it is possible to deliver high quality results. The challenges addressed in this paper may become common challenges for other NASA commercial space efforts. The solutions offered in this paper offer a starting point for overcoming those challenges.

[1] REF for permitting alternate standards:
http://www.nasa.gov/sites/default/files/files/03_Colloredo_International_Standards_Interoperability_CCP.pdf

[2] REF for Exhibit 2 CCP Providers and Suppliers:
http://www.nasa.gov/sites/default/files/files/Mango_CommercialCrewProgram_May2011.pdf

TASC
An Engility Company

Software Assurance Challenges for the Commercial Crew Program

NASA

WVHTC FOUNDATION

Agenda

- Commercial Crew Program (CCP) Overview
- SSO Support
- Software Assurance Challenges
- Questions

Program Overview

- Competitive program to transport crew to/from ISS using commercial services
- Managed at Kennedy Space Center
  - With support from around the Agency
- Highly visible program
  - Attention around the Agency
  - Political/media attention and pressure
- Multiple program phases
  - Different “contract” vehicles (Space Act Agreements, formal contracts)
- Non-traditional Approach
  - Unique acquisition and partnering approach (fosters competition)
  - A set of requirements that focus on what not how

Program Overview

TASC
An Engility Company

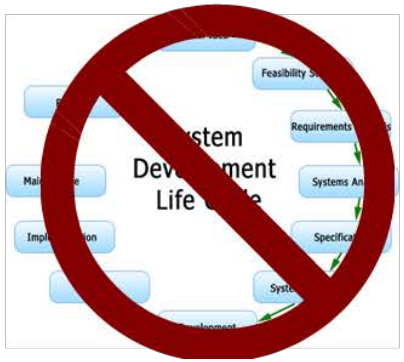
PHASE	DATE	PROVIDERS	CONTRACT TYPE	FOCUS
CCDev1 = Commercial Crew Development Round 1	2010	5	Space Act Agreement	Develop commercial crew transportation concepts and enabling capabilities
CCDev2 = Commercial Crew Development Round 2	2011-2013	4 Funded 3 Unfunded	Space Act Agreement	Design, development, test, review of systems
CCiCap = Commercial Crew Integrated Capability	8/2012-2014	3	Space Act Agreement	Perform tests and mature integrated designs
CPC = Certification Products Contract	12/2012-2014	3	Contract	1) Develop products to implement NASA flight safety and performance requirements; 2) Develop certification plan to achieve safe, crewed missions to the space station
CCtCap = Commercial Crew Transportation Capability -Where we are today-	2014-2017	2	Contract	Final development, testing, verifications to allow crewed demonstration flights to ISS

SSO Support

- SMA Support Office (SSO) is providing software expertise and Software Assurance reach-back support for the CCP SMA team
  - Main support focused on assessing Alternate Standards and Hazard Reports
  - Also supported verification reviews, review boards, etc.
  - Provided support in CCiCap and CPC phases; support to continue through CCtCap phase
  - Comments submitted to program and providers with 99% acceptance rate

Software Assurance Challenges

CCDEV1
CCDEV2
CCiCap
CPC
CCtCap



Atypical Approach

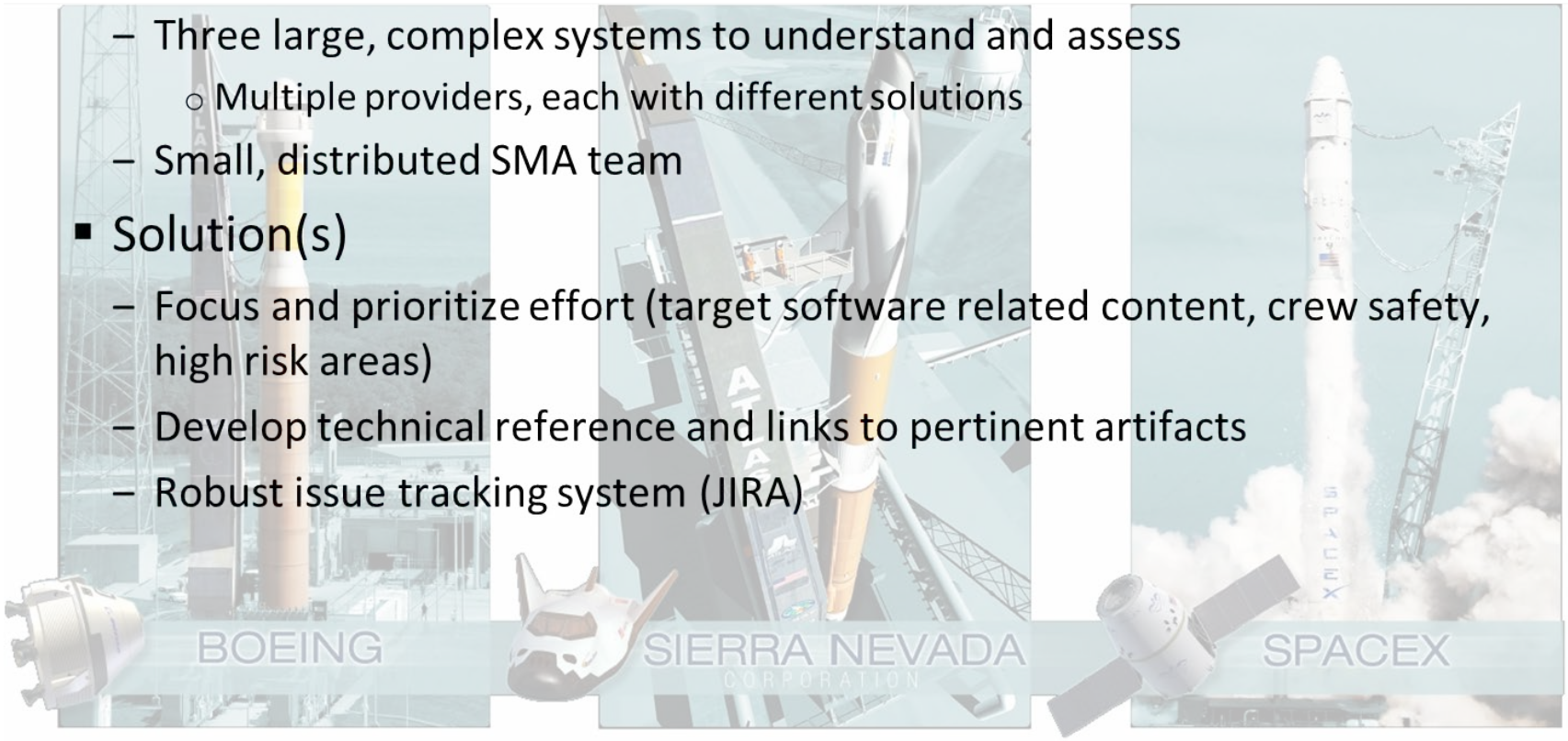
- Challenge: Atypical approach
  - Unique requirements approach (“what” rather than “how”)
  - Allow alternates to NASA standards, including specific waivers
  - Unique provider methods, processes; varying levels of experience working with NASA

- Solution(s)
  - Map provider processes to NASA requirements = understand how NASA’s goals being met (“meet the intent”)
  - Requirement by requirement assessment across artifacts
  - Assess gaps to qualify and communicate risk
    - Be flexible; give providers as much freedom as possible without adding risk to NASA

Large Program, Multiple Commercial Solutions

TASC An Engility Company

- Challenge: Large amount of technical and process information
  - Three large, complex systems to understand and assess
    - Multiple providers, each with different solutions
  - Small, distributed SMA team
- Solution(s)
  - Focus and prioritize effort (target software related content, crew safety, high risk areas)
  - Develop technical reference and links to pertinent artifacts
  - Robust issue tracking system (JIRA)



NASA

WVHTC FOUNDATION

Keeping Proprietary Data Separate

- Challenge: Protecting proprietary data
  - One team providing assurance to multiple providers
  - Cannot cross-pollinate information across providers
  - Core situations: performing analysis and during discussions such as teleconferences, review boards

- Solution(s)
  - Commercial Crew Program limited access to provider data
  - SSO used firewalls and processes to protect data
    - o Point of contact (POC) assigned to each provider
    - o Provider artifacts maintained on CCP repository (not stored locally)
    - o Sensitive data stored in protected locations with restricted access
    - o Separate analysis work products not only from providers, but also our work

Different Funding Methods

- Challenge: Different funding methods (rules of engagement)
  - CCP executing using combination of funding methods
    - o Space Act Agreements and contracts each have different rules: improving product vs. grading; suggestions vs. direction

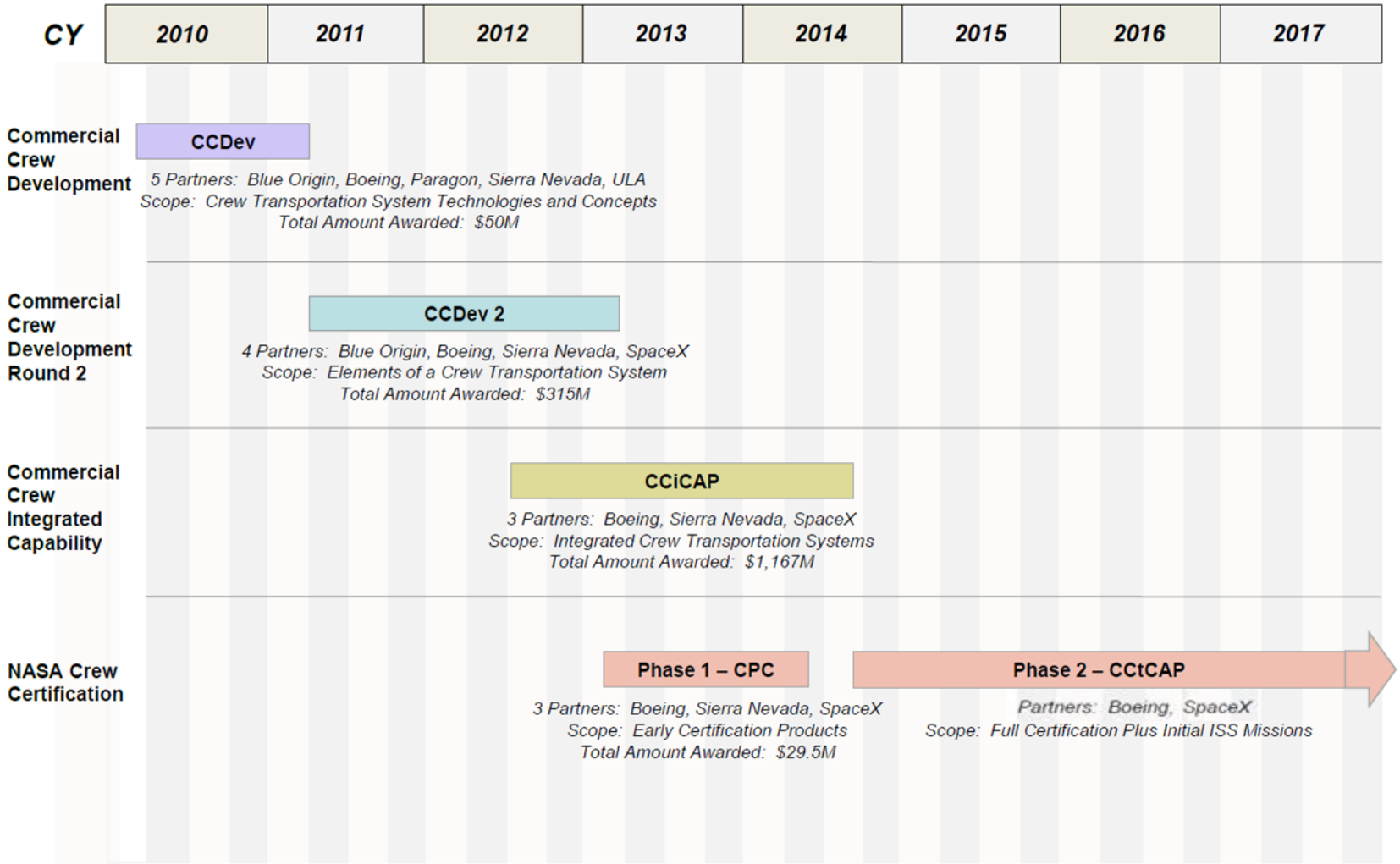
- Solution(s)
  - Rigorous peer review process (SSO and CCP)
    - o Feedback provided to CCP SMA POC to share with provider at his discretion through available channels
  - Robust comment tracking system
    - o Comments phrased as issues and recommendations to support both sets of commenting rules (when appropriate)
  - When in direct communication with providers, ask questions to expose potential defects (rather than stating as issue)

Concurrent Program Phases

- Challenge: Multiple phases executing concurrently
  - Concurrent phases with different rules
  - Artifacts delivered multiple times

- Solution(s)
  - Analysis work products persist across phases
    - o Past comments are verified/updated
    - o Assessment products capture history and current state of artifact
    - o Provide evidence-based assurance (specific references into provider documents as basis for conclusions and findings)
  - Focus assessments on the changes (create compare reports using software tools, etc.)
  - Tailored deliveries to CCP SMA POC based on “rules” for the specific phase

CCP Program Phases

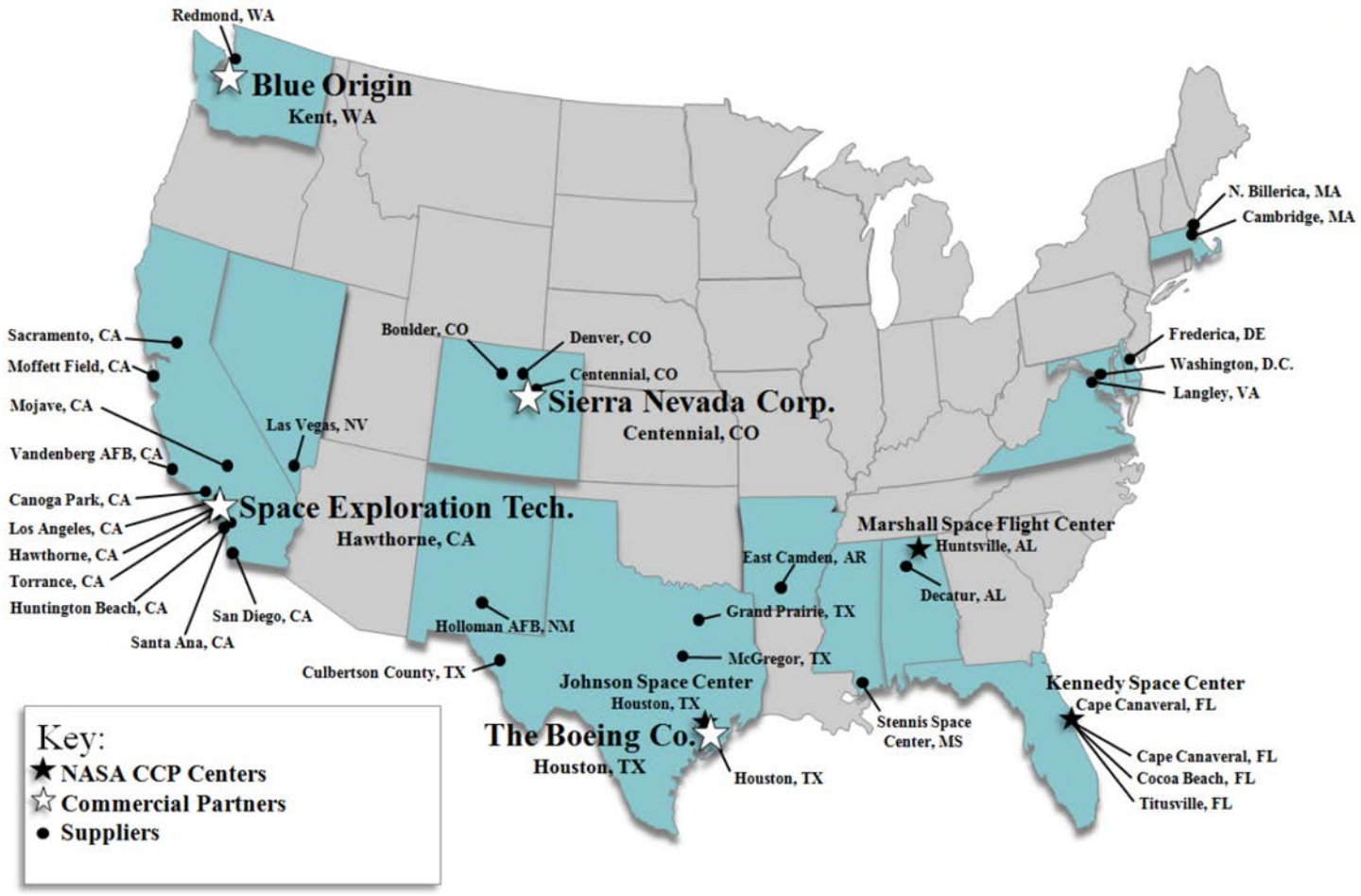


Multiple NASA Stakeholders, Projects

- Challenge: Multiple stakeholders
  - Distributed and diverse stakeholders
  - Other crewed programs have similar requirements/goals
  - Risk of providing inconsistent direction and interpretation of guidance

- Solution(s)
  - Large focus on establishing and maintaining communication (added onsite representative, face to face when possible)
  - Pro-actively identify and pursue potential areas of support
  - Document thought papers to facilitate communication
  - Use pre-determined criteria to keep assessment consistent

CCP Providers and Suppliers



Other Challenges

- Reviews focused on delivered artifacts rather than program goals/standards
- Limited processes/templates to perform assessments
  - Evolving definition for “meets the intent”
  - Initially no process for how to assess hazard reports
- Shortened timeframes
  - Last-minute deliveries from providers
  - Dynamic assignments from the Program

Summary

- Not all of the challenges were unexpected
- Most challenges have been/are being met by using the solutions presented here
- Solutions are shared with the CCP
- In spite of the challenges, SSO has shown it is possible to deliver high quality results.
- These challenges may become common challenges for other NASA commercial space efforts.
- The solutions offered in this presentation offer a starting point for overcoming those challenges.